



WDS2454AP
802.11g WDS/Bridging Wireless LAN
Access Point

User Guide

Regulatory notes and statements

Wireless LAN, Health and Authorisation for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far less than the electromagnetic energy emissions from wireless devices like mobile phones. Wireless LAN devices are safe for use as defined by the relevant frequency safety standards and recommendations. Note: The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board Airplanes
- In an explosive environment
- Where interference risk to other devices or services is perceived or identified as harmful
- In organizations which enforce a policy regarding the use of Wireless LAN devices (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.).

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of additional antennas. The Manufacturer and its authorized resellers/distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the distance between the equipment and the receiver.
3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio/TV technician for help.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with a minimum distance of 20cm between the Antenna and your body. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The antenna(s) used with this device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

C-Tick Compliance

This device is complaint to Australian C-Tick requirements.

TABLE OF CONTENTS

About This Guide	1
Purpose	1
Overview of this User's Guide	1
Unpacking and Setup	2
Unpacking	2
Setup	2
Hardware Installation	3
LED Indicator	3
Rear Panel	3
Hardware connections	4
Connect to the Switch/Hub	4
Check the installation	4
Configuring the Wireless LAN Access Point	5
Login to the Wireless AP through WLAN	5
Login	5
Main Screen of the Access Point	7
Network	8
Security	11
Status	14
Clients	17
Tools	18
Configuration	20
Technical Specifications	21

ABOUT THIS GUIDE

Congratulations on purchasing the WDS2454AP Wireless Access Point. This manual contains detailed instructions on the operation of this product. Please keep this manual for future reference.

With the WDS2454AP Wireless Access Point, wireless enabled devices can share data with each other and with wired LAN devices. The WDS2454AP supports both client and Bridging applications.

WLAN networking can wirelessly transmit and receive data, minimising the need for wired connections, at a speed of up to Fifty-four megabits per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organisation. This mobility provides enhanced productivity to your users.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User Guide

Introduction: Describes the WLAN Access Point and its features.

Unpacking and Setup: Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation: Describes the LED indicators of the AP.

Technical Specifications: Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- ◆ One Wireless Access Point
- ◆ One external power adapter
- ◆ One CD-Rom (User's guide)
- ◆ 2x Antennas (WDS2454AP-A5 only)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Access Point can be performed using the following steps:

- ◆ Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, with line of sight to all of your mobile stations.
- ◆ Visually inspect the Ethernet RJ45 port connector and make sure that it is fully plugged in to the system's Ethernet switch/hub port.
- ◆ Fix the direction of the antennas. Try to place the AP in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
- ◆ Visually inspect the Power Adapter to ensure that it is fully plugged to the devices power jack.

HARDWARE INSTALATION

LED Indicator

PWR/Power

This indicator lights green when the Access Point receives power. Otherwise, it will be off.

LAN (Link/ACT)

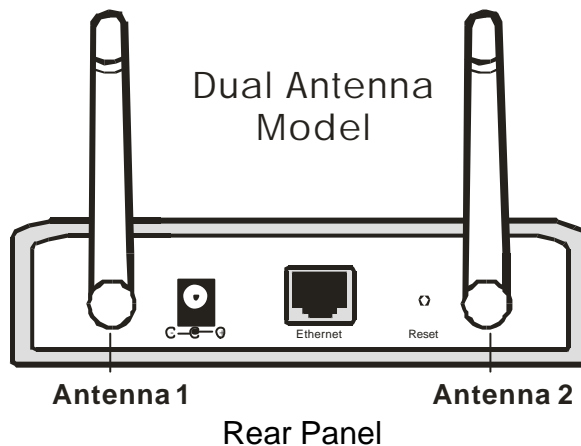
The LED lights green when the LAN port is connected to a 100Mbps Ethernet station, the indicator blinks green while transmitting or receiving data.

WLAN (Link)

The indicator blinks green while the wireless AP is broadcasting packets.

Rear Panel

The figure below shows the rear panel of the Access Point



Ethernet

Ethernet uplink port with 10/100Mbps Fast Ethernet connection, connect this port to a switch/hub.

Reset

The Reset button is used to reset the unit back to factory default. To reset the unit to factory default you will need to hold down the reset button for 10 seconds, the WLAN LED will now turn off. Once the WLAN LED comes back on the unit is ready for use.

The reset button can also be used to reset the Access Point if the unit locks. Just click the reset button once to perform this operation.

DC Power

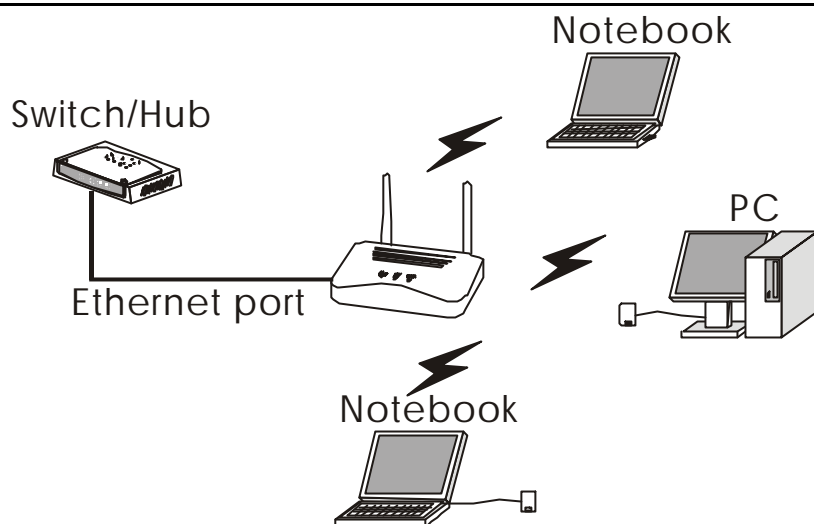
Connect the Power Adapter DC plug to the AP's power jack.

Antenna

There are two antennas connections on the rear panel of the access point.

These connections can be used to connect external high Gain Antennas.

Note: do not over-tighten or cross thread the RSMA connection on the rear of the access point. Doing so could damage the unit, and may void the warranty.



Wireless LAN Networking

Connecting to your office LAN (Switch or Hub)

1. Plug one end of the RJ45 network cable to the Switch/Hub port,
2. Plug the other end of the RJ45 network cable to the Wireless Access Point.
- 3.

Check the installation

The control LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port link LEDs of the unit will light up indicating normal status.
2. If the LAN Port's Link indicator does not light up then check to make sure that the cable has been inserted correctly.

CONFIGURING THE WIRELESS LAN ACCESS POINT

The Wireless Access Point has an easy to use Web GUI interface for configuration. The AP can be configured through a Web Browser. A network manager can manage, control and monitor the AP from the local LAN. This section indicates how to configure the AP.

Login to the Wireless AP through WLAN

Before configuring the Wireless AP through a wireless client, make sure that the SSID, Channel and the WEP key have been configured correctly.

The default settings of the Wireless AP are:

SSID: default

Channel: 6

WEP Encryption: disabled

Login

When configuring this device through the Ethernet port please ensure that your computer is set to the same IP range. For example, the default IP address of the AP is **192.168.1.100** and the manager PC should be set to 192.168.1.x (where x is a number between 1 and 254), and the default subnet mask is 255.255.255.0.

Open Internet Explorer 5.0 or above Web browser.

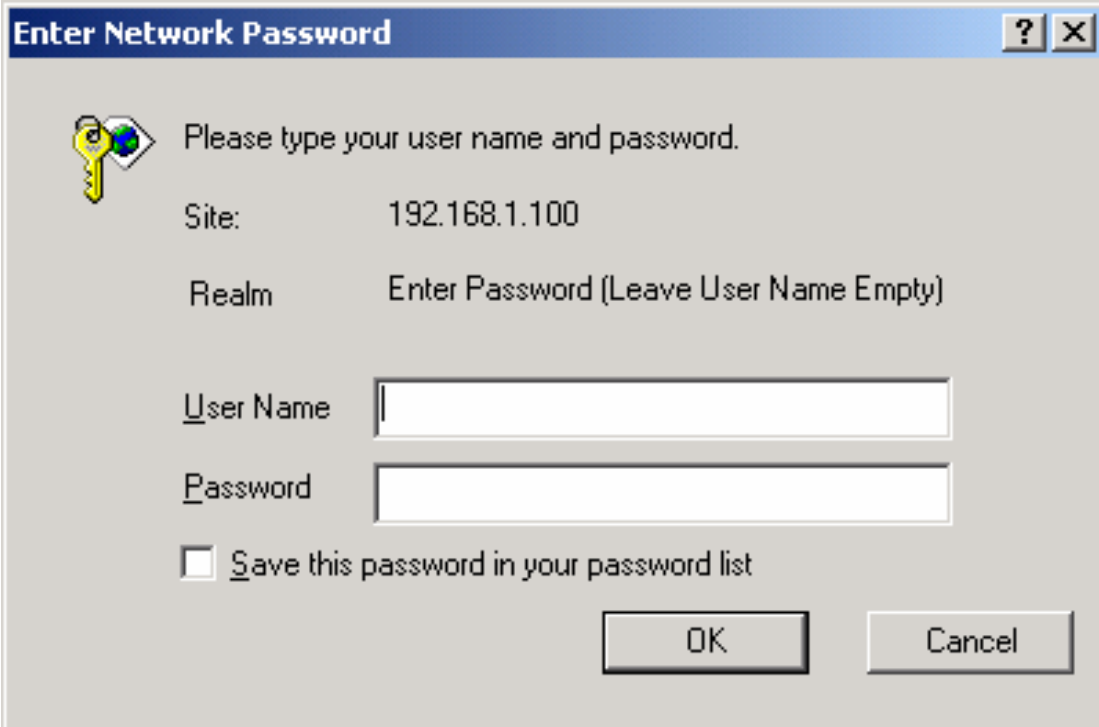
Enter the IP address **http://192.168.1.100** (the factory-default IP address setting) in the address location.




If you have configured a username and password for the access point you will be prompted with a login box when you enter the IP address in to the web browser.

Enter the appropriate username and password and hit enter.

Note: by default there is no username and password set in to the device.



Enter Network Password [?] [X]

 Please type your user name and password.

Site: 192.168.1.100

Realm: Enter Password (Leave User Name Empty)

User Name:

Password:

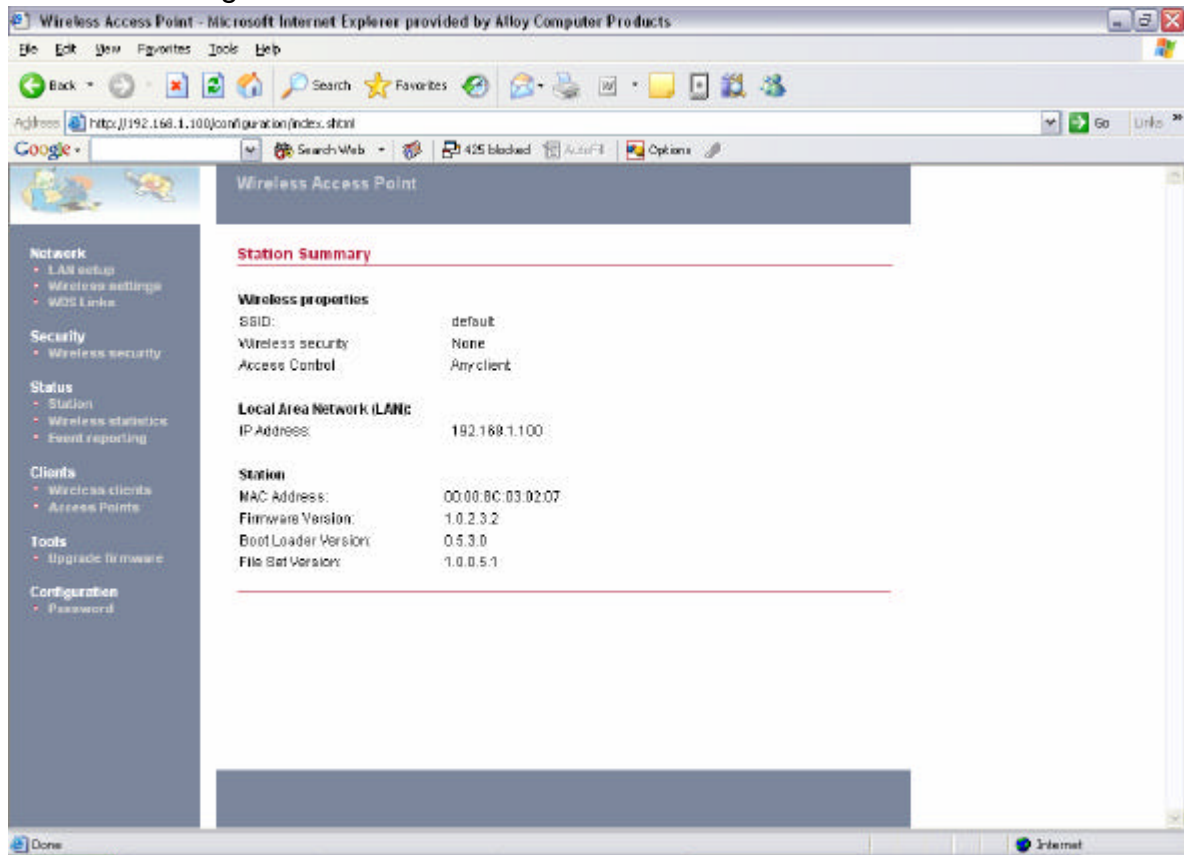
Save this password in your password list

OK Cancel

Main Screen of the Access Point

The first screen that appears in the browser is the station summary page.

There are six main functions included on the left side of the main screen: Network, Security, Status, Clients, Tools and Configuration.



Network

The Network Section is used to configure the IP address of the unit, Wireless settings and the WDS Links of the Access Point.

I. LAN Setup

The LAN Setup function is used to configure the basic LAN settings:

Dynamic (DHCP Client): Select Dynamic for dynamic IP address allocation from a DHCP Server.

Static IP: Select Static to configure an IP Address, Subnet Mask and Gateway for the Access Point.

Local Area Network (LAN)

Primary Address Selection

Dynamic

Static IP

IP Address

Subnet mask

Gateway

II. Wireless Settings

The wireless settings screen contains two sections **Radio Settings** and **Wireless LAN**.

Wireless Settings

Radio settings:

Regulatory Domain: FCC [change region...](#)

Wireless LAN:

Wireless network name (SSID):

Band: 2.4 GHz (Mixed) [change policy...](#)

Radio Channel:

Broadcast SSID:

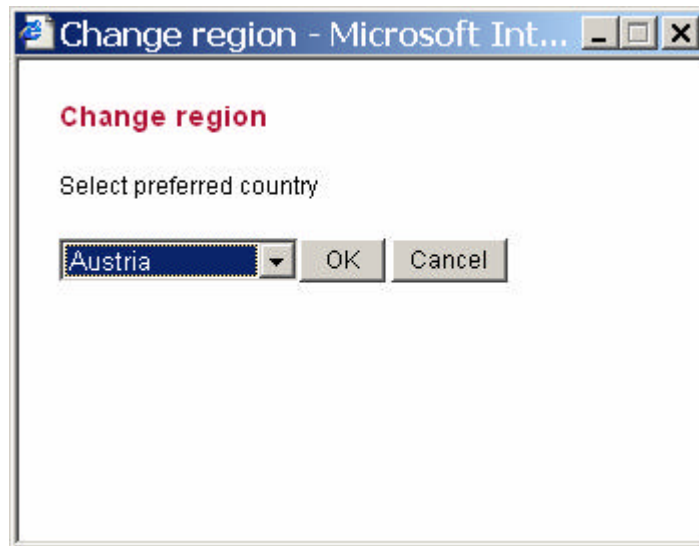
Radio Settings: to configure the Regulatory Domain settings.

➤ **Regulatory Domain:** Please select the appropriate regulatory domain for your country.

Radio settings:

Regulatory Domain: ETSI [change region...](#)

Click on the “change region” button and a window will pop out, select the region in which you are using this AP.

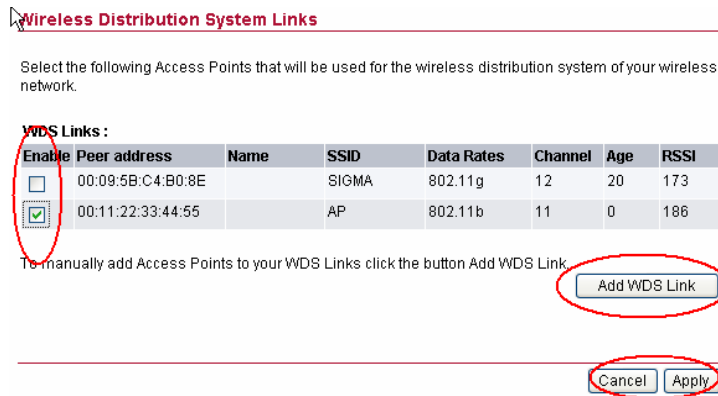


Wireless LAN Settings: to configure the wireless network settings.

- **Wireless Network Name (SSID):** SSID is an ASCII string up to 32 characters that is used to identify the WLAN and prevents the unintentional merging of two co-located WLANs. The SSID value must be the same in all stations and AP's in the extended WLAN.
- **Band:** you can select to change the radio band to mixed mode, G-only or B-only, a window will pop up to change the policy.
 - Mixed mode:** Supports both 802.11g and 802.11b clients.
 - G-only:** Only supports 802.11g clients.
 - B-only:** Only supports 802.11b clients.
- **Radio Channel:** there are 14 channels available due to different Regulatory Domains. The channels differ from country to country; select the channel to be used.
- **Broadcast SSID:** when this function is enabled the access point will not broadcast the units SSID to wireless clients.

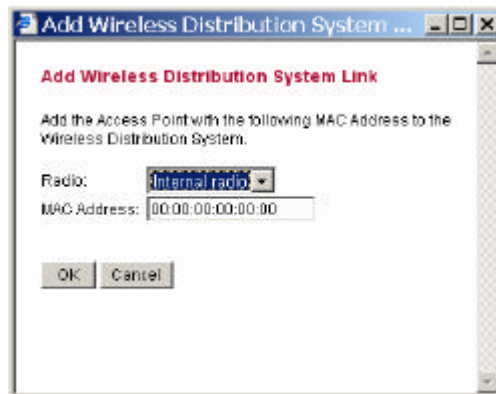
III. WDS Links

WDS (Wireless Distribution System) uses wireless bridging to communicate with other APs. When you enter the WDS screen a list of available AP's will appear. To create a WDS link with a particular Access Point click enable on the left side of the screen and click apply to add the AP to your WDS Link, or click the "Add WDS Link" button to add the APs that you need to add.



The WDS Link will scan and find all available access points running within a range of 3 channels. If your access point is not found automatically there are two other ways to add an AP to your WDS link.

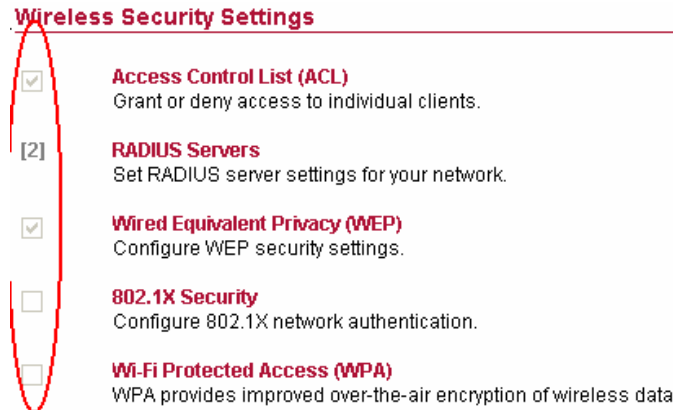
1. Click the "Add WDS Link" button, a window will appear, type in the MAC address of the AP that you need to communicate with.
2. Change your AP radio channel within the range of 3 channels to scan for the AP that you want to connect to.



To remove an AP from the WDS Link list, unclick the enable dialog box to remove the WDS Link. In Addition, make sure you configure all WDS APs to work on the same radio channel and with the same security settings.

Security

The WDS2454AP provides a range of security features used to prevent unauthorised access to your wireless network. These security features include, WPA, 802.1x and WEP.



If a particular security feature has been enabled a tick box or a number will be displayed next to the corresponding security feature.

- Check sign means that the function is enabled.
- The numbers show how many Radius servers have been configured.

I. Access Control List

The Access Control List is used to limit access to the AP from certain wireless clients. When enabled only wireless clients who's MAC address is listed are able to communicate with the Access Point.

- **Default Access:** Select Accept to allow access to the unit from the list of MAC addresses, or select Reject to block access to the unit from all listed MAC addresses.
- **Specific Clients:** Add all MAC addresses of wireless clients who's access you want to control.

Access Control List

Enable access control list

Default Access

Accept Reject

Specific Clients

MAC Address	Access
00:0F:0E:01:23:45	accept
	<input type="button" value="Add..."/> <input type="button" value="Delete..."/>

II. Radius Server

A RADIUS server is used to authenticate the connection for clients and return authentication key parameters to the users to connect to the wireless network.

RADIUS (Remote Authentication Dial-In User Service) utilises a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

Re-authentication Time: Enter a time in seconds that users will have to re-authenticate with the RADIUS server.

RADIUS Servers

Reauthentication Time: seconds

IP Address	Port Number
11.12.13.14	1812

Click the “Add” button to add the Radius Server IP Address, Server UDP port and Shared Secret. The shared secret is used to allow communication between the AP and the RADIUS Server.

Add RADIUS Server

Add the Access Point with the following IP Address, UDP Port and Secret.

IP Address:

UDP Port:

Secret:

III. Wired Equivalent Privacy (WEP)

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

When selecting WEP encryption, click the “Use WEP Security” to enable the WEP security function.

- ◆ **64-bits:** selecting the 64bit, you must type 10 values in the following range (0~F, hexadecimal).
- ◆ **128-bits:** selecting the 128bit, you must type 26 values in the following range (0~F, hexadecimal).

Wired Equivalent Privacy (WEP)

Use WEP security
Pre-shared Key:
 64-bits
 128-bits

IV. 802.1x Security

To address the shortcomings of WEP for authentication, the industry is working towards solutions based on the 802.1x specification, which is based on the Extensible Authentication Protocol (EAP). EAP was designed with flexibility in mind, and it has been used as the basis for a number of network authentication extensions.

Click to enable the 802.1x security function.

802.1X Security

Use 802.1X security
Key Size
 64-bits
 128-bits
Group Key Rekey Settings
 No rekeying
 Rekey every minutes
 Rekey every x 1000 packets

- ◆ **Key Size:** select either 64bit or 128-bit for the key size of the 802.1x security.

- ◆ **Group Key Setting:**

No Rekeying: the clients will not need to re-key the password to authenticate with the Radius Server.

Rekeying Time: Type in the time in minutes when clients will need to re-key the password for authentication and security.

Rekeying packets: Type in the amount of packets that will be transmitted before clients will need to re-key the password for authentication and security.

V. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is the newest and most reliable standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilises a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilises a symmetric 128-Bit block data encryption.

- **Disable WPA Security:** to disable the WPA security.

- **Use WPA with Pre-Shared Key:** type in 8 ~ 63 characters inside the dialog box to setup the WPA password used between the AP and the clients.
- **Use WPA with Radius Server:** the authentication between the Radius Server, the AP and the clients using the Group Key Re-key Settings.
 - No Rekeying:** the clients will not need to re-key the password to authenticate with the Radius Server.
 - Rekeying Time:** Type in the time in minutes when clients will need to re-key the password for authentication and security.
 - Rekeying packets:** Type in the amount of packets that will be transmitted before clients will need to re-key the password for authentication and security.
- **Update Group Key:** to update the password when the station or the client leaves the Networking Group (BSS, Basic Service Set).

Wi-Fi Protected Access (WPA)

Disable WPA security
 Use WPA with pre-shared key
 Password Phrase (8-63 characters)

Use WPA with RADIUS server
 Group Key Rekey settings:

- No rekeying
- Rekey every minutes
- Rekey every x 1000 packets
- Update Group Key if station leaves BSS

Status

This function will show the statistics of the Station, Wireless Statistics and Event Reporting.

I. Station

This screen will show the status summary of the system.

Station Summary

Wireless properties

SSID:	PM11G
Wireless security	Wep
Access Control	Any client

Local Area Network (LAN):

IP Address:	169.254.16.4 172.16.5.145
-------------	------------------------------

Station

MAC Address:	00:30:B4:82:10:04
Firmware Version:	1.0.0.1
Boot Loader Version:	0.5.3.0
File Set Version:	1.0.0.1

II. Wireless Statistics

This screen shows the statistics of the wireless AP.

Wireless Statistics

	Wireless LAN
Transmitted Fragments	0
Transmitted Multicasts	0
Transmitted Frame Count	903450
Failed Packets	0
Retry Count	0
Multiple Retry Count	0
Duplicate Frames	0
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	0
Received Fragment Count	0
Received Multicasts	118
FCS Errors	2843990
WEP Undecryptable	0

III. Event Report

This screen shows all events that have occurred on the AP, press “Reset Event Log” to clear the record of the events.

Event reporting

The following events are reported by the Access Point:

Reset eventlog

Report level	Facility	ID	Description	Count	Occurence
Info	System	102	802.1x authenticator started	1	00m 00d 14:15:12
Notice	System	109	Respawning paed	1	00m 00d 14:15:12
Info	System	104	802.1x authenticator stopped	1	00m 00d 14:15:07
Alert	Kernel	10C	Kernel: <1>offset in paed: 0x0033e8c4	1	00m 00d 14:15:07
Alert	Kernel	10C	Kernel: <1>Brk: 0x0 - 0x0	1	00m 00d 14:15:07
Alert	Kernel	10C	Kernel: <1>Bss: 0x0 - 0x0	1	00m 00d 14:15:07

Clients

This function shows the list of the wireless clients connected to the AP.

I. Wireless Clients

This function shows the list of wireless clients that are connected to the AP.

Wireless Clients

Wireless clients

Address	Rate	Quality	RSSI	State	Age
00:05:4E:46:70:BF	24		-38	Forwarding	1

II. Access Points

This function shows the list of Wireless Access Points that the AP can connect to, this is the list that you can use for WDS Links, refer for the WDS Links on page 10.

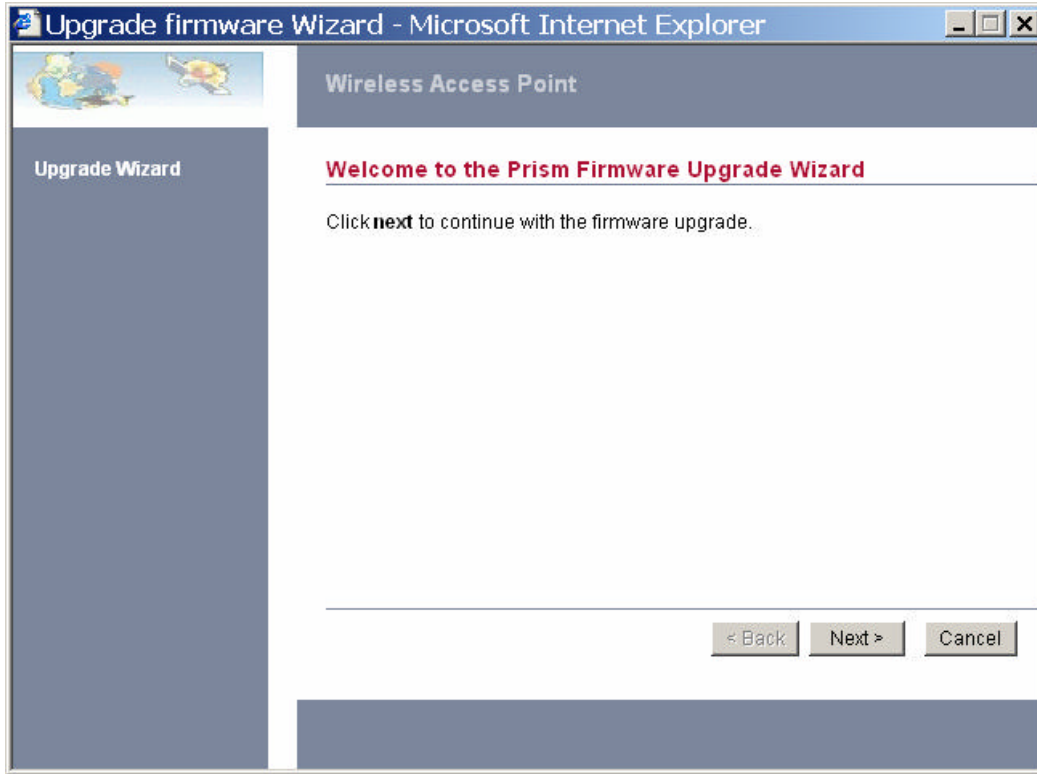
Access Points

Detected Access Points

BSSID	SSID	Data Rates	Channel	Age	RSSI
00:0000:82:12:50	default	11 5.5 2 1	6	0	176
00:0000:82:1E:6D	SALES	11 5.5 2 1	7	0	163
00:0000:AB:CD:EF	CalvinAP	11 5.5 2 1	9	0	168
00:0000:00:44:2A	default	11 5.5 2 1	6	33	170

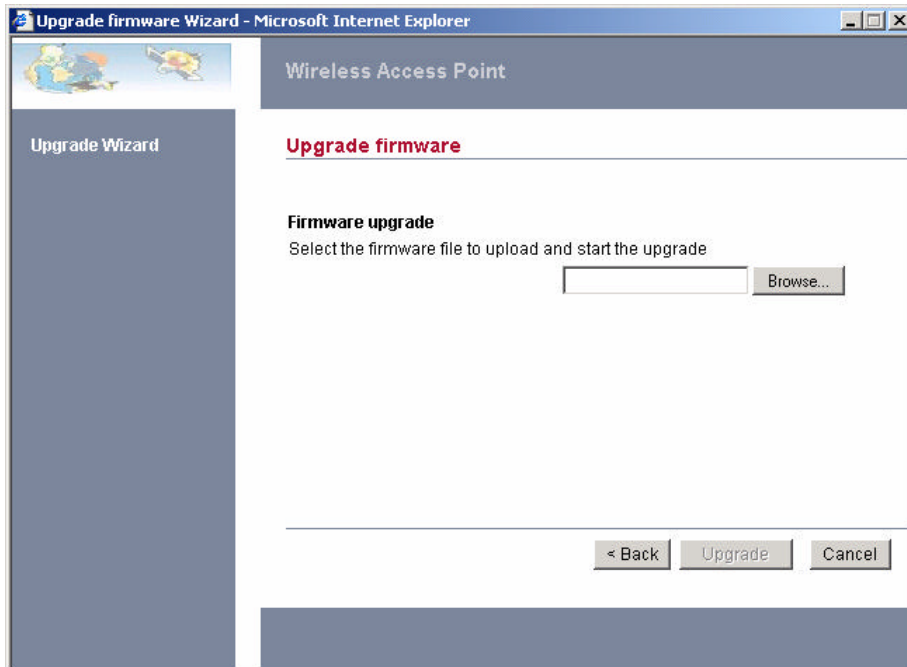
Tools

This function will help you to upgrade the firmware of the AP, press the “Upgrade Firmware” button in the left side of the menu screen and a window will appear as shown below.



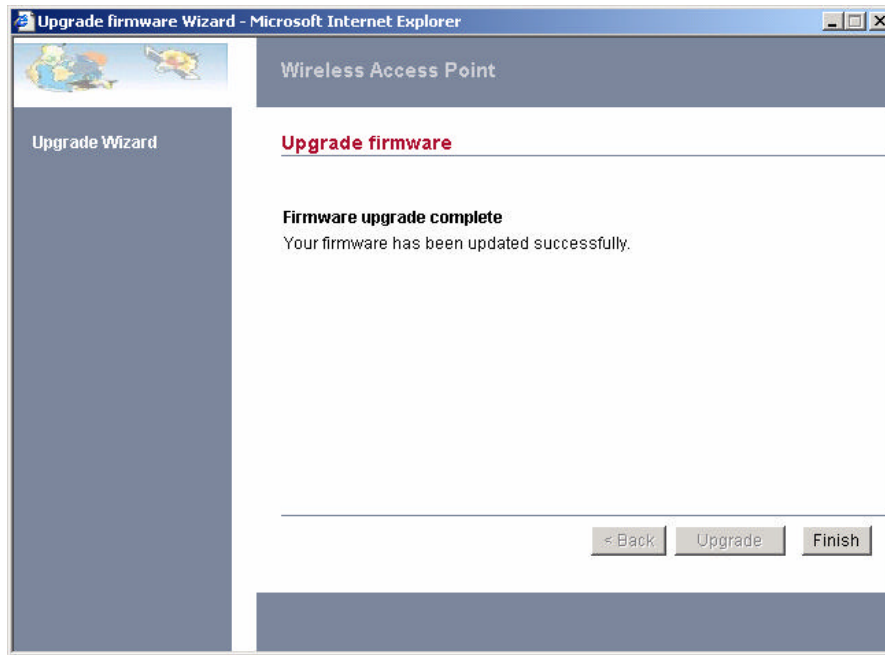
Press “Next “.

Type the firmware file that you need to upgrade inside the dialog box, or press the “Browse” button to find the firmware file location.



Press the “Upgrade” button to proceed with the upgrade procedure.

When uploading the file to the AP, **do not power off the AP until the “Firmware Upgrade Complete” screen appears.**



Press the “Reset” button on the rear panel of the AP, to reset to unit back to factory default.

I. Change Password

This function will help you to configure the password of the AP, type in the new password inside the New password and Confirm password dialog box, press the “Change password” button to activate this function.

Security Against Unauthorized Configuration

Change password

Set the password needed to access and configure your Access Point.

New password: (3-16 characters)

Confirm password:

II. Lock Access Point

Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it, press the reset button on the rear panel of the AP to unlock.

Lock Access Point

Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it.

TECHNICAL SPECIFICATIONS

General	
Standards	Standard: IEEE 802.11g IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type:	OFDM (Orthogonal Frequency Division Multiplexing)
Modulation:	QPSK / BPSK / CCK / OFDM
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Frequency Band:	2.4 GHz
Channel:	1 ~ 11 Channels (US, Canada, China) 1 ~ 13 Channels (Europe) 1 ~ 14 Channels (Japan)
Data Encryption:	64 bit / 128 bit WEP Encryption, WPA
Data Transfer Rate	Fast Ethernet: 100Mbps Wireless: Up to 54Mbps (with Automatic Scale Back)
Receiver Sensitivity	54Mbps: Typical -68dBm @10% PER 11Mbps: Typical -81dBm @8% PER
Transmit Power	802.11g: Minimum 12dBm typically 802.11b: Minimum 15dBm typically
Transmission Range:	Outdoor: 100~300M (depends on environment) Indoor: 50~100M (depends on environment)
Network Cables	10BASET: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna: (WDS2454AP-A5 only)	2 x 5dBi Dipole Antenna
Physical and Environmental	
DC inputs	DC 5V /1.2A
Power Consumption	3W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	140 x 98 x 30 mm (W x H x D) without Antenna
Compliance:	FCC Class B, CE Mark B, C-Tick